A24 Cont.

a cipher engine adapted to transparently encrypt and decrypt at least one data stream flowing between the data generating device and the data storage device on command from said main controller.

Please cancel claim 22.

REMARKS

Status of Claims

Claims 1-21, inclusive, have been amended, as indicated hereinabove. Claim 22 has been canceled. No new claims have been added. Therefore, the claims presently under consideration are 1-21, inclusive.

Amendments to Specification

The specification has been amended to correct typographical, syntactic and grammatical errors without adding new subject matter, as indicated hereinabove.

Amendments to Drawings

Figures 1 – 5 have been amended pursuant to MPEP 608.02(t), 608.02(v), and 37 C.F.R. 1.84(o), as indicated in Exhibits A and B, attached hereto. No new subject matter has been introduced by the amendments to Figures 1 – 5.

Conclusion

In view of the above amendments and remarks, Applicant respectfully requests consideration of amended claims 1 – 21, and the issuance of a Notice of Allowability in respect to claims 1 – 21, inclusive.

The Commissioner is hereby authorized to charge any fee which should have been filed herewith to our PTO Deposit Account No. 50-2577. A duplicate copy of this paper is enclosed. Please show our above-referenced docket number with any credit or charge to the deposit account.

Attached hereto is a marked-up version of the changes made to the specification and claims by the instant preliminary amendment. The attached page is captioned "**Version with markings to show changes made**."

Date: October 21, 2003

Respectfully submitted,

By _____
Natu J. Patel, Esq.
Registration No.: 39559
Attorney for Applicant

Wang & Patel, P.C.
1301 Dove Street, Suite 1050
Newport Beach, CA 92660
Tel. (949) 833-8483
Fax (949) 833-2281
PTO Customer No. 37819

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE SPECIFICATION:

The original title appearing on page 1 and page12 has been amended as follows:

--[An encryption-decryption device for date storage] CRYPTOGRAPHIC DEVICE--

The sub-heading on page 1, line 3, has been amended as follows:

--[1. Field of the Invention] FIELD OF THE INVENTION--

The paragraph beginning on page 1, line 4 and ending on page 1, line 7 has been amended as follows:

--The present invention relates [to an encryption-decryption device for data storage and in particular relates to a data encryption-decryption device provided on the data path connecting a data-generating device and a data storage device to accomplish the purpose of encryption-decryption.] generally to cryptography and more particularly to a device adapted to perform data encryption/decryption without compromising the overall system performance.--

The sub-heading on page 1, line 9 has been amended as follows:

--[2. Background of the Invention] BACKGROUND OF THE INVENTION--

The paragraph beginning on page 1, line 10 and ending on page 1, line 25 has been amended as follows:

--[In the present day of Internet Communications and Electronic Commerce, most businesses and personal matters, are carried out on public communication routes. When important or secret information is transmitted and received on these routes, or] Encryption is a security technology designed to preserve the privacy and confidentiality of sensitive data that is being stored or transmitted. Sensitive data is routinely stored [in media without encryption, the risks of unauthorized data access and interception exist. When secrecy and security cannot be assured, the needs for data encryption arise. Data encryption provides a

mechanism for protecting data from being unlawfully obtained on storage media or communication routes. In other words, encryption is the process of converting original data to data of incomprehensible form. Being the reverse process of encryption, decryption involves the operation of transforming the encrypted data back to its original fashion. In actual application, data is converted to incomprehensible form before being transmitted on communication routes (e.g., Internet or Local Area Network) or kept in storage media. After completing the decryption process on encrypted data, authorized users obtain usable data in its original form.] unencrypted on desktop computers, workstations, notebooks, personal digital assistants (PDAs), cellular telephones, and the like. The hard drives of notebooks are especially at risk as the computers are frequently used in non-secure environments and may be relatively easily removed by an unauthorized user. Computer hard drives may contain strategic data, patent applications, patent drawings, litigation documents, consumer lists, private health care information, payroll data and other types of sensitive data. Users frequently store unencrypted passwords and access codes to corporate networks on notebooks, which may compromise corporate network security. Statistics compiled annually by the FBI show that network security breaches are to a significant extent being perpetrated by employees or contractors who have or can gain access to sensitive data on an intranet. Moreover, unattended desktop PCs become frequent targets for unauthorized users attempting to gain illicit entry into a private network.--

The paragraph beginning on page 1, line 26 and ending on page 2, line 12 has been amended as follows:

--[A schematic of the prior art encryption is shown in FIG. 1. Data storage and access are executed between a Hard Disk and a Central Processing Unit (CPU). Without processing power of the CPU 2, Encryption Software 3 alone cannot perform the encryption process. As a result, CPU 2 compromises its performance by allocating operational resources per instructions of the Encryption Software 3. To improve the performance of the CPU 2, conventional remedy normally involves adding an acceleration chip 4 between CPU 2 and Encryption Software 3. Since the acceleration chip 4 is not part of the CPU 2, it would require additional cost of purchasing and mounting the acceleration chip 4 on circuit board to raise the performance of the CPU 2. In addition, the necessity for loading Encryption Software 3 on CPU 2 decreases capability thereof, slow down or incapacitate CPU 2 from executing encryption and, consequently, causes inconvenience of using Encryption Software

3, especially when expendable resource or operational performance of the CPU 2 is insufficient. It becomes desirable to find solutions to improve the deficiency.] Comparatively few cryptographic applications have been developed to protect data, with most of the applications being software-based applications adapted to perform file-level cryptography. File-level cryptography can also be done by various hardware devices such as PCMCIA cards or external ASIC-based devices. On the surface, encrypting only selected files instead of entire hard drives seems to make sense since not all data is confidential. However, file cryptography is inherently slow because the entire file must be decrypted before any portion of the file can be presented to the user. Also, file encryption normally ignores the temporary and swap files that are automatically created and stored in clear text on the hard drive. Worse still, file encryption frequently results in compromised overall system performance, and requires manual intervention by users who may become confused and frustrated by the number of requisite interactive steps embedded in the application. From an organizational point of view, the lack of automatic and transparent cryptographic operation makes it inherently difficult to enforce data security policies on computers, mobile communication devices and networks alike. Furthermore, the level of security attainable with file-level cryptography is questionable, since file encryption programs run under the control of the computer operating system (OS) and the OS lacks sufficient access control. If an unauthorized user were capable of subverting the OS, subverting the file-level cryptography application would be entirely feasible as well. Although PCMCIA encryption cards and external ASIC encryption devices have been designed to provide greater key security and to improve performance, these devices have had only marginal success and suffer from a variety of compatibility issues. It, therefore, becomes increasingly clear that conventional cryptography applications are not suitable for organizations and/or individuals requiring optimized security, convenience and uncompromised system performance.--

The paragraph beginning on page 2, line 13 and ending on page 2, line 16 has been deleted in its entirety.

The sub-heading on page 2, line 18 has been amended as follows:

--[Summary of the Invention] SUMMARY OF THE INVENTION--

The paragraph beginning on page 2, line 19 and ending on page 2, line 22 has been amended as follows:

--[An object of the] The present invention is [to provide a data encryption-decryption] generally directed to a cryptographic device [(an IC chip, for instance) for data encryption-decryption such that great improvement is attained when host system resources are relieved of the encryption-decryption process] adapted to perform data encryption and decryption on at least one data stream flowing between at least one data generating device and at least one data storage device without compromising overall system performance.--

The paragraph beginning on page 2, line 23 and ending on page 3, line 2 has been amended as follows:

--[Another object] In one embodiment of the present invention, [is to provide a hardware] the cryptographic device [for allowing direct flow of data and command, on the data path connecting the host] is adapted to intercept at least one data stream flowing between the data generating device and the data storage device, [such that the existence of the data encryption-decryption device is unknown to either the host or the data storage device.] and transparently perform data encryption and decryption in accordance with the intercepted data stream. [Since the host, the data encryption-decryption device and the storage device are substantially connected serially. From the host's viewpoint, the data encryption-decryption device is regarded as the data storage device. Thus, as far as data interface and communication is concerned, the data encryption-decryption device is invisible. Therefore, compatibility problems do not exist.]--

The paragraph beginning on page 3, line 3 and ending on page 3, line 10 has been amended as follows:

--[The third object] In another embodiment of the present invention, [is to provide a device capable of making intelligent decisions for distinguishing the types of data received. One example is, if Command or Control signals are detected, the device understands that encryption or decryption would not be required. Whereas, when Data signals are received, the device knows as well that encryption or decryption is to be executed. The devices' decision capability relieves the host from making above decisions, thereby elevating the operational efficiency.] the cryptographic device comprises a data stream interceptor, a main controller receiving input from the data stream interceptor, a data generating controller adapted to

perform at least one data transfer protocol with the data generating device on command from the main controller, a data storage controller adapted to perform at least one data transfer protocol with the data storage device on command from the main controller, and a cipher engine adapted to transparently encrypt and decrypt data streams flowing between the data generating device and the data storage device on command from the main controller.--

The paragraph beginning on page 3, line 11 and ending on page 3, line 13 has been deleted in its entirety.

The paragraph beginning on page 3, line 14 and ending on page 3, line 19 has been deleted in its entirety.

The paragraph beginning on page 3, line 21 and ending on page 3, line 22 has been amended as follows:

--These and other aspects of the present invention will become apparent from a review of the accompanying drawings and [T]the following detailed [D]description [and Designation of Drawings are provided in order to help understand the features and content] of the present invention.--

The sub-heading on page 3, line 24 has been amended as follows:

--[Brief Description of the Drawings] BRIEF DESCRIPTION OF THE DRAWINGS--

The paragraph beginning on page 3, line 25 and ending on page 3, line 26, has been amended as follows:

--The invention is best understood from the following detailed description when read in conjunction with the accompanying drawings [form a material part of this description,]. It is emphasized that, according to common practice, the various features of the drawings are not to scale with dimensions of the various features being arbitrarily expanded or reduced for clarity. Like numerals denote like features throughout the specification and drawings in which:--

The paragraph beginning on page 3, line 27 and ending on page 3, line 28 has been amended as follows:

--[FIG. 1 is a schematic block diagram of prior art encryption in accordance with the present invention.] Figure 1 schematically depicts a cryptographic device operatively coupled between a data generating device and a data storage device for use during data transfer;--

The paragraph beginning on page 3, line 29 and ending on page 4, line 2, has been amended as follows:

--[FIG. 2 is a schematic block diagram showing the relationship between Data-generating Device, Data Encryption-Decryption Device and Data Storage Device in the first embodiment of the present invention.] Figure 2 schematically depicts a data storage device with an integral cryptographic device operatively coupled to a data generating device for use during data transfer;--

The paragraph beginning on page 4, line 3 and ending on page 4, line 5, has been amended as follows:

--[FIG. 3 is a schematic block diagram showing the relationship between Data-generating Device, Data Encryption-Decryption Device and Data Storage Device in the second embodiment of the present invention.] Figure 3 schematically depicts a data generating device with an integral cryptographic device operatively coupled to a data storage device for use during data transfer; and--

The paragraph beginning on page 4, line 6 and ending on page 4, line 8, has been amended as follows:

--[FIG. 4 is a schematic block diagram showing the relationship between Data-generating Device, Data Encryption-Decryption Device and Data Storage Device in the third embodiment of] Figure 4 schematically depicts the architecture of a cryptographic device in accordance with the present invention.--

The paragraph beginning on page 4, line 9 and ending on page 4, line 11, has been deleted in its entirety.

The sub-heading on page 4, line 13 has been amended as follows:

--[Detailed Description of the Preferred Embodiment] DETAILED DESCRIPTION OF THE INVENTION--

The paragraph beginning on page 4, line 14 and ending on page 4, line 21 has been amended as follows:

--Some embodiments of [T]the present invention [relates to an encryption-decryption device for data storage and in particular relates to a data encryption-decryption hardware device provided serially on the data path connecting a data-generating device and a data storage device for accomplishing encryption-decryption process. The Encryption-Decryption Device provides a novel encryption-decryption construction for improved data encryption (and decryption) and universal system adaptation without comprising the overall system performance.] are described in detail with reference to the related drawings of Figures 1 - 4. Additional embodiments, features and/or advantages of the invention will become apparent from the ensuing description or may be learned by practicing the invention.--

The paragraph beginning on page 4, line 22 and ending on page 5, line 7, has been amended as follows:

--[As shown in Figure 2, the first embodiment of the present invention is a data encryption-decryption device located on the data path. Being an encryption-decryption device serially provided on the data path connecting a data storage device 11 and a data-generating device 13, the data encryption-decryption device 12 serves as a bridge connecting the data storage device 11 and the data-generating device 13. The data encryption-decryption device 12 is capable of performing the encryption-decryption operations independently without utilizing resources of the] Figure 1 schematically depicts a cryptographic device 12 operatively coupled between a data generating device 13 and a data storage device 11 for use during data transfer. In general, data generating device 13 may be a desktop/notebook computer, microprocessor, hub, router, mobile computing device, interface card, or any other device capable of generating data, while data storage device 11 may be a computer hard drive, tape drive, floppy diskette, compact disk drive, magnetic optical drive, digital video recorder, flash memory card, magnetic tape, compact disk (CD), CD-RW, CD+RW, CD-R, digital versatile disk, PCMCIA card, or any other device capable of storing data for retrieval purposes. Cryptographic device 12 is adapted to perform data encryption/decryption during

data transfers between data generating device 13 and data storage device 11 without compromising the overall system performance. Specifically, cryptographic device 12 does not utilize resources typically associated with data[-]generating device 13, such as CPU, DRAM, or other system resources[.] during data transfers between data generating device 13 and data storage device 11. From the functional viewpoint of [the] data generating device 13 [storage device 11, the data encryption-decryption device 12 is regarded as a virtual data-generating device 13. Similarly, from the viewpoint the data-generating device 13, the data encryption-decryption device 12 is treated as a virtual] and/or data storage device 11, data transfers are being performed directly between data generating device 13 and/or data storage device 11, respectively, without any intervention by cryptographic device 12. In general, cryptographic device 12 acts as an "invisible" data transfer bridge connecting data generating device 13 and data storage device 11. [As far as data interface and communication is concerned, the data encryption-decryption device is invisible. Therefore, data communication between these two devices will function without hindrance.] Cryptographic device 12 may be implemented in any suitable stand-alone hardware form such as a hub or the like. Cryptographic device 12 may also be implemented as a designated data transfer interface adapted to use various data communication protocols in network applications such as local area networks (LANs), wide area networks (WANs), and the like.--

The paragraph beginning on page 5, line 8 and ending on page 5, line 18, has been deleted in its entirety.

The paragraph beginning on page 5, line 19 and ending on page 6, line 6, has been amended as follows:

--[As shown in Figure 3, the second embodiment of the present invention is a data encryption-decryption device being placed on the data path. In this embodiment, a data encryption-decryption] Figure 2 schematically depicts a data storage device 21 with an integral cryptographic device 22 being operatively coupled to a data generating device 23 for use during data transfer. Cryptographic device 22 [in IC] may be integrated in ASIC chip form [is installed serially] on the front end of the [designated outgoing transmission] data transfer interface [inside a] (not shown) of data storage device 21 [(e.g. Hard Disk, Floppy Disk, Flash Memory Card, Digital Video Recorder or CD-RW, etc) such that the control hardware and drivers or the data storage device 21 require no design change. In] without any

modification of dataflow control hardware, drivers or data storage device 21 itself. The data transfer interface may be in the form of Socket, IDE, PCI, 1394, SCSI, PCMCIA, [or] USB[,] [etc., the designated outgoing transmission interface allows encryption and decryption of data transmitted between the data storage device 21 and the data-generating device 23. As shown in Figure 4, the third embodiment of the present invention is a data encryption-decryption device being placed on the data path. In this embodiment, a data encryption-decryption device 32, in IC chip form as well, is installed serially on the front end of the designated outgoing transmission interface, inside a data-generating device 33 (e.g. Host, Notebook, Microprocessor, Flash Memory Card and Interface Card, etc.). In the socket form of IDE, PCI, 1394, SCSI, PCMCIA or USB, etc., the designated outgoing transmission interface allows encryption and decryption of data transmitted between the data storage device 31 and the data-generating device 33.] or any other suitable data transfer interface. In general, data generating device 23 may be a desktop/notebook computer, microprocessor, hub, router, mobile computing device, interface card, or any other device capable of generating data. Data storage device 21 may be a computer hard drive, tape drive, floppy diskette, compact disk drive, magnetic optical drive, digital video recorder, flash memory card, magnetic tape, compact disk (CD), CD-RW, CD+RW, CD-R, digital versatile disk, PCMCIA card, or any other device capable of storing data for retrieval purposes. Cryptographic device 22 is programmed to perform transparently data encryption/decryption during data transfers between data generating device 23 and data storage device 21 without compromising the overall system performance. From the functional viewpoint of data generating device 23, data transfer is being performed directly with data storage device 21 without any apparent intervention by integral cryptographic device 22.--

The paragraph beginning on page 6, line 7 and ending on page 6, line 18, has been amended as follows:

--[The embodiments in Figures 2 through 4 demonstrate that many varieties of combination can be adopted by the present invention. The data encryption-decryption device, m one example, may be a stand-alone hardware device such as a hub, provided between a data-generating device and a data storage device. It may be, in other examples, installed inside a data-generating device or a data storage device. And can be compatible to] Figure 3 schematically depicts a data generating device 33 with an integral cryptographic device 32 being operatively coupled to a data storage device 31 for use during data transfer.

Cryptographic device 32 may be integrated in ASIC chip form on the front end of the data transfer interface (not shown) of data generating device 33 without any modification to dataflow control hardware, drivers or data generating device 33 itself. The data transfer interface may be in the form of Socket, IDE, PCI, 1394, SCSI, USB[, or other communication] or any other suitable data transfer interface.[, it may also act as a designated interface adapting various communication protocols. Therefore, the scope of application for the present invention ranges from the basic data encryption between a single host and its peripheral storage media to those involving connection and communication on the Local Area Networks (LANs) and the Internet.] In general, data generating device 33 may be a desktop/notebook computer, microprocessor, hub, router, mobile computing device, interface card, or any other device capable of generating data. Data storage device 31 may be a computer hard drive, tape drive, floppy diskette, compact disk drive, magnetic optical drive, digital video recorder, flash memory card, magnetic tape, compact disk (CD), CD-RW, CD+RW, CD-R, digital versatile disk, PCMCIA card, or any other device capable of storing data for retrieval purposes. Cryptographic device 32 is programmed to perform transparently data encryption/decryption during data transfers between data generating device 33 and data storage device 31 without compromising the overall system performance. From the functional viewpoint of data storage device 31, data transfer is being performed directly with data generating device 33 without any apparent intervention by integral cryptographic device 32.--

The paragraph beginning on page 6, line 19 and ending on page 7, line 1, has been amended as follows:

--[Figure 5 shows a detailed construction of the Data Encryption-Decryption Device in a preferred embodiment of] Figure 4 depicts schematically the architecture of a cryptographic device 43 in accordance with the present invention.[, where a data encryption-decryption device is placed on the data path connecting] In the embodiment of Figure 4, cryptographic device 43 is shown operatively coupled between a data[-] generating device 41 and a data storage device 42[, an interceptor 431 is provided such that its one end is connected with said data path and its other end is connected to the main control 432, said main control 432 is electrically connected to a data-generating control device 433, a data storage control device 434 and a data encryption-decryption engine 436, said data encryption-decryption engine 436 is so arranged that its one end is serially connected to an input buffer 435 which in turn is connected to a data-generating device 41, and its other end is serially

connected to an output buffer 437 which in turn is connected to a data storage device 42. In addition, the data-generating control device 433 is electrically connected to the data-generating device 41 and the data storage control device 434 is electrically connected to the data storage device 42.] for use during data transfer. In general, data generating device 41 may be a desktop/notebook computer, microprocessor, hub, router, mobile computing device, interface card, or any other device capable of generating data. Data storage device 42 may be a computer hard drive, tape drive, floppy diskette, compact disk drive, magnetic optical drive, digital video recorder, flash memory card, magnetic tape, compact disk (CD), CD-RW, CD+RW, CD-R, digital versatile disk, PCMCIA card, or any other device capable of storing data for retrieval purposes. Cryptographic device 43 may be implemented in any suitable hardware form. Cryptographic device 43 is adapted to perform transparently data encryption and decryption during data transfers between data generating device 41 and data storage device 42 with no impact on overall system performance.--

The paragraph beginning on page 7, line 2 and ending on page 7, line 31, has been amended as follows:

--[Based on the above configuration, said main control 432 determines whether incoming data, generated in the data-generating device 41 and subsequently intercepted by the] As generally illustrated in Figure 4, cryptographic device 43 comprises a data stream interceptor 431 which is operatively coupled to a main controller 432. Main controller 432 communicates control signals to a data generating controller 433, a data storage controller 434, and a cipher engine 436. Main controller 432 receives input from data stream interceptor 431[,] and determines whether an incoming data stream, which may include command/control and/or data signals, is to be encrypted, [(or] decrypted[)] or [allowed to pass. Accordingly, the Command or Control Signals are allowed to pass and transmit to the data storage device without encryption. When the data-generating control device 433, the data storage control device 434 and the data encryption-decryption engine 436 are notified of the incoming data, the data-generating control device 433 transmits or receives a Control Signal and act as an interface between the data encryption-decryption device and the data-generating device 41. In other words, communication mode is determined by the interface of the data-generating device 41. For instance, if the data-generating device 41 is a Host and is using IDE interface for communication, IDE protocol will be the communication mode. On the other hand, if the host is equipped with and is using the PCI interface, PCI protocol will

become the communication mode. Similarly, as the data storage control device 434 transmits or receives a Control Signal and act as an interface between the data encryption-decryption device and the] passed through unmodified. In this regard, data stream interceptor 431 is adapted to distinguish between command/control and data signal transfers. Specifically, interceptor 431 is configured to pass through certain command/control signals via a bypass data path 44, and intercept other command/control signals which are transmitted to main controller 432, as generally depicted in Figure 4. Main controller 432 instructs data generating controller 433 and data storage controller 434 to perform specific data transfer protocols such as read/write, PIO/DMA, ATA/IDE, PCI, and the like with corresponding peer controllers (not shown) of data generating device 41 and data storage device 42, [various communication modes are involved when designated data is being encrypted or decrypted in response to Control Signals of the main control 44. An input] respectively, according to the intercepted command/control signals. Main controller 432 also transmits control signals to cipher engine 436 to notify the same of an incoming data stream. Cipher engine 436 is operatively coupled between an input buffer 435 and an output buffer 437, and programmed to transparently encrypt/decrypt streaming data during data transfer between data generating device 41 and data storage device 42, as generally shown in Figure 4. Input buffer 435 [and an output buffer 437 are provided between the encryption-decryption engine 436 and the data-generating device 41 between the data encryption-decryption engine 436 and the data storage device 42, for storing] stores pre-encrypted [or decrypted data] and pre-decrypted [or encrypted] data, [respectively. Said data buffers are also capable of converting the data length. The data-] while output buffer 437 stores encrypted and decrypted data, respectively. Input buffer 435 receives data from data generating device 41 or data storage device 42 depending on the type of data transfer. Output buffer 437 outputs data to data generating device 41 or data storage device 42 depending on the type of data transfer. Data generating device 41 [usually has] may include a 1-bit, 8-it, 16-bit[,] or 32-bit data width interface[, or 64-bit interface, The input buffer 435 converts incoming data from the data-generating device 41 for encryption and, after encryption, the output buffer 437 then transforms the encrypted data for storage in the data storage device 42]. Data storage device 42 may include a 1-bit, 8-bit, 16-bit or 32-bit data width interface. Cipher engine 436 may include a 64-bit, 128-bit or other data width interface depending on the ciphering algorithm being used. Input buffer 435 is adapted to convert incoming data width to a data width suitable for input to cipher engine

436. Output buffer 437 is adapted to convert incoming data width to a data width suitable for output to data storage device 42 or data generating device 41.--

The paragraph beginning on page 7, line 32 and ending on page 8, line 16, has been amended as follows:

--[To recap, the present invention discloses a data encryption-decryption device serially provided on the data path connecting a data-generating device and a data storage device for encryption-decryption purpose. Since resources of the data-generating device is not involved in the operation, the data encryption-decryption device is capable of accomplishing data encryption-decryption] No resources associated with data generating device 41 or data storage device 42, or any other system resources, are being used by cryptographic device 43 during data transfer between data generating device 41 and data storage device 42. Cryptographic device 43 independently and transparently encrypts/decrypts incoming data streams without compromising the overall system performance. [By providing corresponding interface capabilities to accommodate both the data-generating device and data storage device, the data encryption-decryption device is transparent to the data-generating devices and data storage devices. Additionally, by adopting suitable data transmission protocols and interface, between the data-generating devices, data encryption-decryption device and data storage devices, as designated interface, the present invention allows the scope of application to extend from encryption between the host and the peripheral storage media to those involving connection and] A person skilled in the art would recognize that cryptographic device 43 may be adapted for implementation in network communication [on the] applications such as those involving LANs, WANs, virtual private networks (VPNs), and the Internet. [It is apparent that the present invention discloses novel configurations and provides inventive steps over the prior arts.]--

The paragraph beginning on page 8, line 17 and ending on page 8, line 21, has been amended as follows:

--While the invention has been described in terms of [several preferred] various specific embodiments, [various alternatives and modifications can be devised by] those skilled in the art [without departing from invention. Accordingly, the present invention is intended to embrace all such alternatives that fall within the scope of the claims.] would recognize that the invention can be practiced with modification within the spirit and scope of

the claims. Additionally, features illustrated or described as part of one embodiment can be used in another embodiment to provide yet another embodiment such that the features are not limited to the specific embodiments described hereinabove. Thus, it is intended that the present invention cover all such embodiments and variations as long as such embodiments and variations come within the scope of the appended claims and their equivalents.--

The sub-heading on page 12, line 3, has been amended as follows:

--[Abstract] ABSTRACT OF THE DISCLOSURE--

The paragraph beginning on page 12, line 4 and ending on page 12, line 15, has been amended as follows:

[By incorporating a data encryption-decryption] A cryptographic device [on the data path connecting a data-generating] comprises a data stream interceptor, a main controller receiving input from the data stream interceptor, and a pair of data generating and storage controllers adapted to perform data transfer protocols with corresponding peer controllers of a data generating device and a data storage device, [an encryption-decryption device for data storage is disclosed. Input instruction coming from the data-generating device determines whether encryption (or decryption) is to be carried out. If encryption (or decryption) is not called for, data is forwarded directly to a storage device and no encryption process (or decryption process) will be performed. When encryption (or decryption) is required, encryption process (or decryption process) will be executed on the data encryption-decryption] respectively, on command from the main controller. The cryptographic device further comprises a cipher engine [provided within the data encryption-decryption device. The encryption-decryption] programmed to transparently encrypt and decrypt data streams flowing between the data generating device and data storage device on command from the main controller. The cryptographic device [provides a novel encryption-decryption construction for improved data encryption (and decryption) without compromising the overall system performance.] does not utilize system resources associated with the data generating and storage devices during operation.

IN THE CLAIMS:

Claims 1-21, inclusive, have been amended as follows:

1 (Amended). [An encryption-decryption] A cryptographic device [capable of encrypting] adapted to perform data encryption and [decrypting incoming data, comprising: a data-generating control] decryption on at least one data stream flowing between at least one data generating device [capable of communicating with an external data-generating device; a data storage control device capable of communicating with an external data storage device; a data encryption-decryption device for providing encrypting and decrypting functions; and a control device respectively connecting with the data-generating control device, the data storage control device and the data encryption-decryption device for controlling the same, said control device being capable to determine whether said incoming data need to be encrypted or decrypted by said data encryption-decryption device] and at least one data storage device without compromising the overall system performance.

2 (Amended). [The] A cryptographic device [of claim 1, wherein the data-generating] adapted to perform data encryption on at least one date stream flowing between at least one data generating device [is a host computer] and at least one data storage device without compromising overall system performance.

3 (Amended). [The] A cryptographic device [of claim 1, wherein the data-generating] adapted to perform data decryption on at least one data stream flowing between at least one data generating device [is a notebook computer] and at least one data storage device without compromising overall system performance.

4 (Amended) [The] A cryptographic device [of claim 1, wherein the data-generating] adapted to intercept at least one data stream flowing between at least one data generating device [is a microprocessor] and at least one data storage device, and transparently perform data encryption in accordance with said at least one intercepted data stream.

5 (Amended) [The] A cryptographic device [of claim 1, wherein the data-generating] adapted to intercept at least one data stream flowing between at least one data generating device [is an interface card] and at least one data storage device, and transparently perform data encryption in accordance with said at least one intercepted data stream.

6 (Amended) [The] A cryptographic device [of claim 1, wherein the data-generating] adapted to intercept at least one data stream flowing between at least one data generating device [is a router] and at least one data storage device, and transparently perform data encryption in accordance with said at least one intercepted data stream.

7 (Amended) [The] A cryptographic device [of claim 1, wherein the] comprising:

at least one data stream interceptor;

a main controller receiving input from said at least one stream interceptor;

at least one data generating controller adapted to perform at least one data transfer protocol with at least one data generating device on command from said main controller;

at least one data storage controller adapted to perform at least one data transfer protocol with at least one data storage device [is a hard disk] on command from said main controller; and

at least one cipher engine adapted to transparently encrypt at least one data stream flowing between said at least one data generating device and said at least one data storage device on command from said main controller.

8 (Amended) The cryptographic device of claim [1,] 7, wherein [the data storage device is a floppy disk] said at least one cipher engine is operatively coupled between at least one input buffer and at least one output buffer.

9 (Amended) The cryptographic device of claim [1,] 8, wherein [the data storage device is a CD] said at least one input buffer receives data from said at least one data generating device and said at least one data storage device.

10 (Amended) The cryptographic device of claim [1,] 8, wherein [the data storage device is a Magnetic Optical Drive] said at least one output buffer outputs data to said at least one data generating device and said at least one data storage device.

11 (Amended) [The] A cryptographic device, [of claim 1, wherein the] comprising:

at least one date stream interceptor;

a main controller receiving input from said at least one data stream interceptor;

at least one data generating controller adapted to perform at least one data transfer protocol with at least one data generating device on command from said main controller;

at least one data storage controller adapted to perform at least one data transfer protocol with at least one data storage device [is a Digital Video Recorder] on command from said main controller; and

at least one cipher engine adapted to transparently decrypt at least one data stream flowing between said at least one data generating device and said at least one data storage device on command from said main controller.

12 (Amended) The cryptographic device of claim [1] 11, wherein [the data storage device is a Flash Memory Card] said at least one cipher engine is operatively coupled between at least one input buffer and at least one output buffer.

13 (Amended) The cryptographic device of claim [1] 12, [further comprising an interceptive device connecting with the main control, said interceptive device being capable of intercepting incoming data for determining if said incoming data need to be encrypted or decrypted by said data encryption-decryption device] wherein said at least one input buffer receives data input from said at least one data generating device and said at least one data storage device.

14 (Amended) The cryptographic device of claim [1] 12, [further comprising a data] wherein said at least on output buffer [connected between the] outputs data to said at least one data [encryption-decryption] generating device and [the data-generating] said at least one data storage device.

15 (Amended) [An encryption-decryption] A cryptographic device [connecting with a data storage device and a data-generating] comprising:

at least one data stream interceptor;

a main controller receiving input from said at least one data stream interceptor;

at least one data generating controller adapted to perform at least one data transfer protocol with at least one data generating device [via predetermined interfaces, wherein said data encryption-decryption device is a hardware device serially connected between the] on command from said main controller;

at least one data storage controller adapted to perform at least one data transfer protocol with at least one data storage device [and the data-generating device for acting as a bridge for data transmitting there between, said data encryption-decryption device further including a control device and a data encryption-decryption] on command from said main controller; and

at least one cipher engine adapted to transparently encrypt and decrypt at least one data stream flowing between said at least one data generating device [for encrypting and decrypting] and said at least [part of the] one data storage device on command from said main controller.

16 (Amended) The cryptographic device of claim 15, wherein said [data-generating device is a device choosing from a group consisting of host computer, notebook computer, microprocessor, interface card, and router] at least one cipher engine is operatively coupled between at least one input buffer and at least one output buffer.

17 (Amended) The cryptographic device of claim [15] 16, wherein said at least one input buffer receives data from said at least one data generating device and said at least one data storage device [is a device choosing from a group consisting of hard disk, floppy, CD, Flash Memory Card, MO, Digital Video Recorder and PCMCIA].

18 (Amended) The cryptographic device of claim [15] 16, wherein said [data encryption-decryption device is an IC chip provided within the data-generating] at least one

output buffer outputs data to said at least one data generating device and said at least one data storage device.

19 (Amended) [The] A cryptographic device [of claim 16, wherein said data encryption-decryption device is serially provided on a front end of the interface located in the data-generating] operatively coupled between a data generating device and a data storage device for use during data transfer, said cryptographic device comprising:

a data stream interceptor;

a main controller receiving input from said at least one data stream interceptor;

a data generating controller adapted to perform at least one data transfer protocol with the data generating device on command from said main controller;

a data storage controller adapted to perform at least one data transfer protocol with the data storage device on command from said main controller; and

a cipher engine adapted to transparently encrypt and decrypt at least one data stream flowing between the data generating device and the data storage device on command from said main controller.

20 (Amended) [The] A cryptographic device [of claim 15, wherein said data encryption-decryption device is an IC chip provided] integrated within [the] a data storage device for use during data transfer with a data generating device, said cryptographic device comprising:

a data stream interceptor;

a main controller receiving input from said data stream interceptor;

a data generating controller adapted to perform at least one data transfer protocol with the data generating device on command from said main controller;

a data storage controller adapted to perform at least one data transfer protocol with the data storage device on command from said main controller; and

a cipher engine adapted to transparently encrypt and decrypt at least one data stream flowing between the data generating device and the data storage device on command from said main controller.

21 (Amended) [The] A cryptographic device [of claim 20, wherein said data encryption-decryption device is serially provided on a front end of the interface located in the] integrated within a data generating device for use during data transfer with a data storage device, said cryptographic device comprising:

a data stream interceptor;

a main controller receiving input from said data stream interceptor;

a data generating controller adapted to perform at least one data transfer protocol with the data generating device on command from said main controller;

a data storage controller adapted to perform at least one data transfer protocol with the data storage device on command from said main controller; and

a cipher engine adapted to transparently encrypt and decrypt at least one data stream flowing between the data generating device and the data storage device on command from said main controller.

Claim 22 has been canceled.

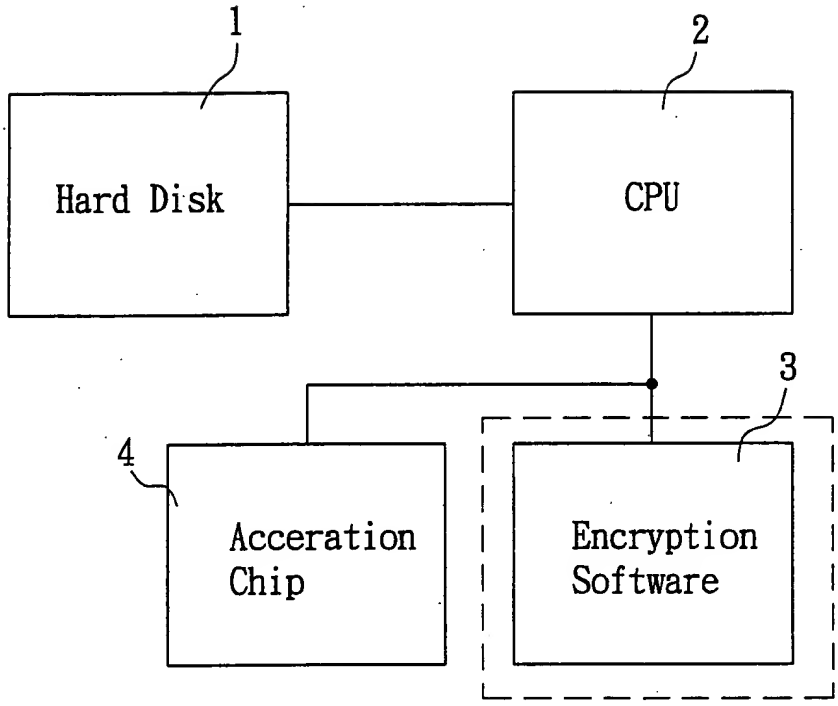

FIG. 1
(PRIOR ART)
(CANCELED)

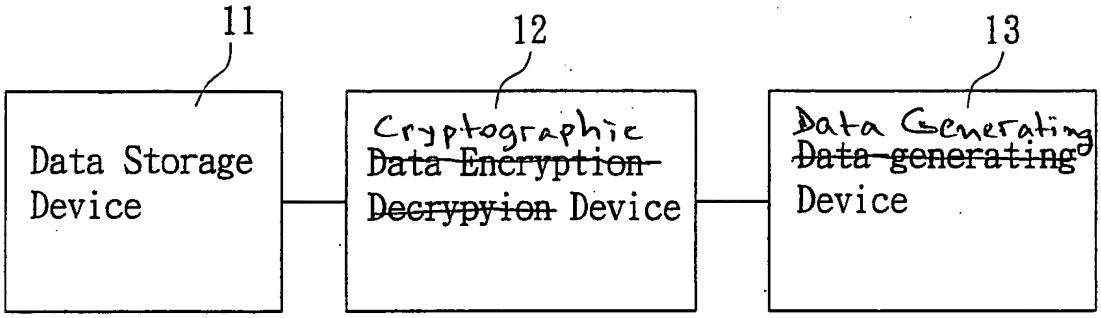

FIG. 2 1

(AMENDED)

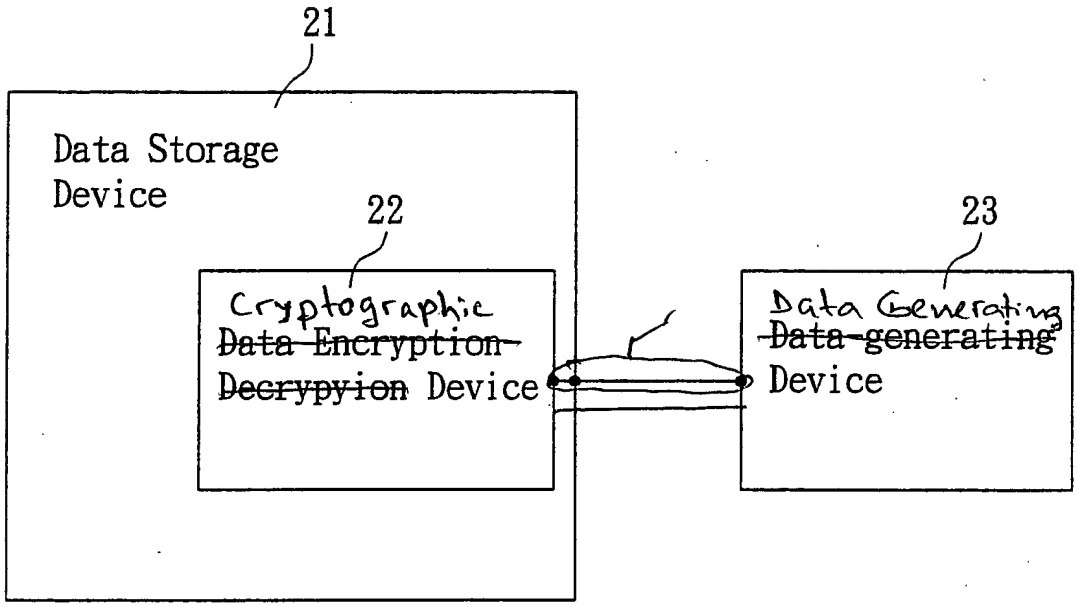

FIG. 32
(AMENDED)

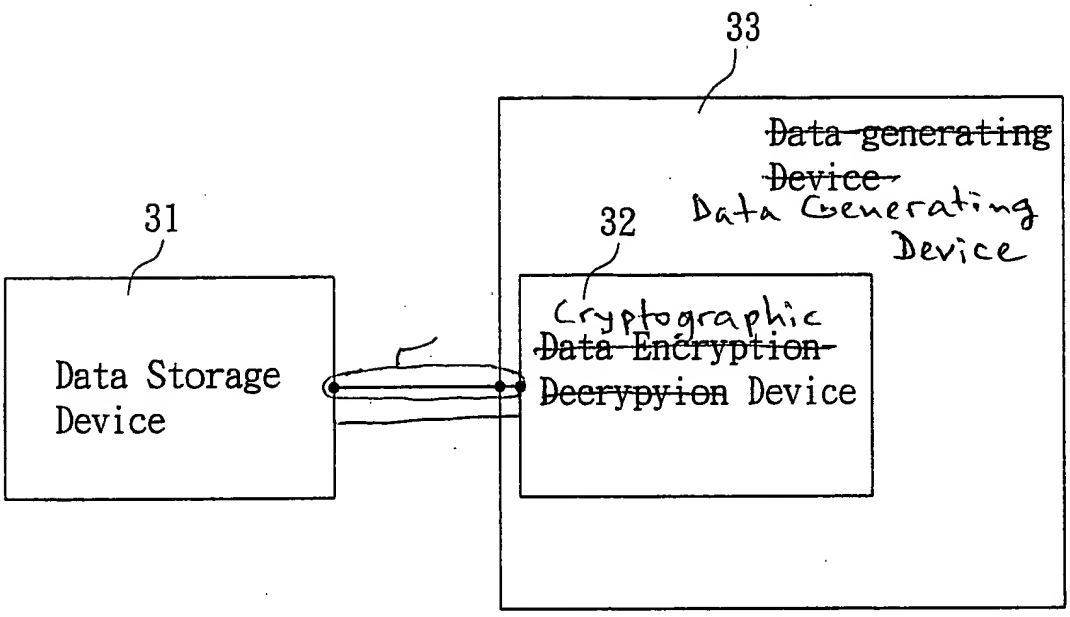

FIG. 3
(AMENDED)

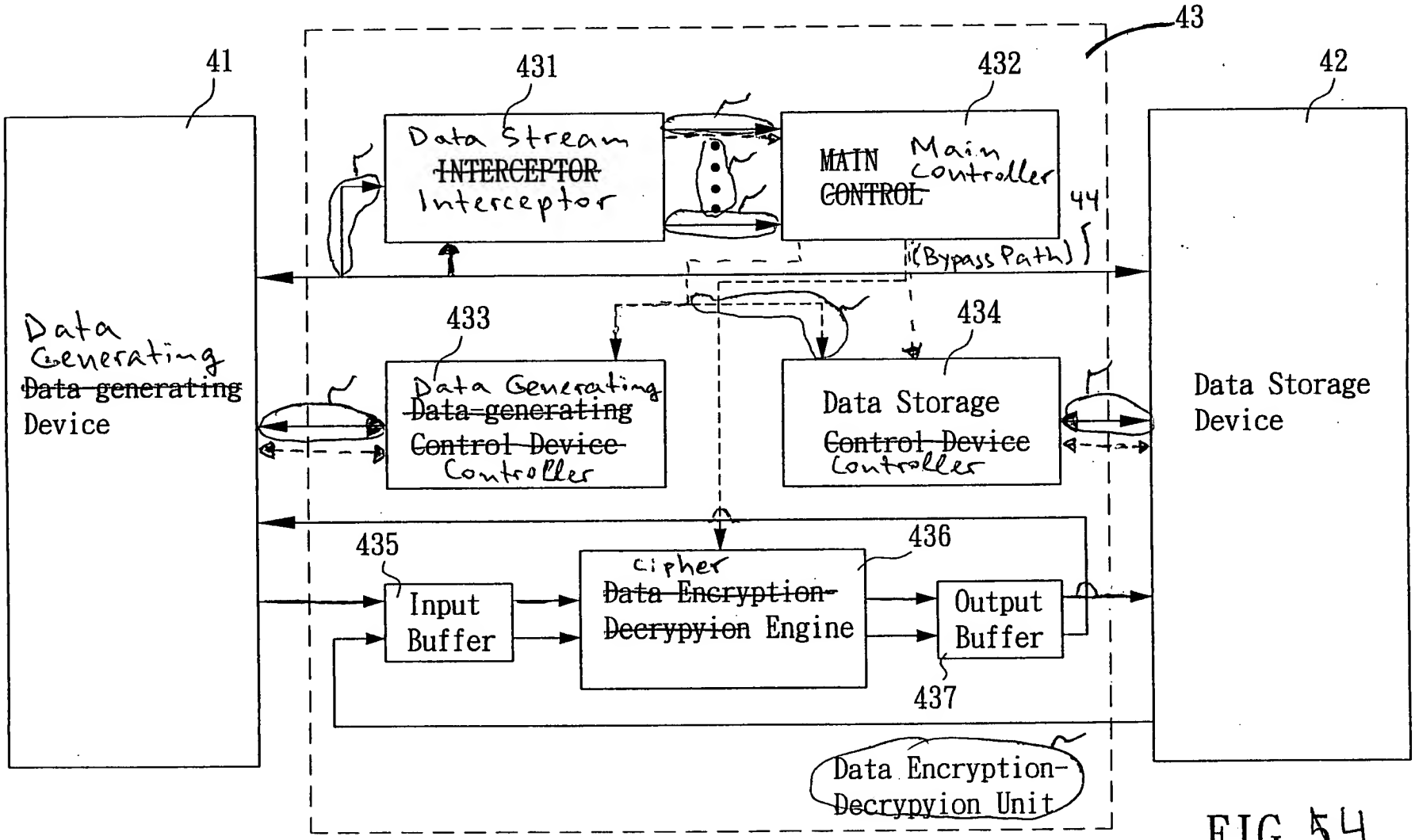

FIG. 5A
(AMENDED)